21-MJ-4032-DHH
21-MJ-4035-DHH
21-MJ-4036-DHH

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANTS

I, Lisa A. Crandall, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the FBI since June 2010 and I am currently assigned to the Boston Division, Lakeville Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to, among other things, the online sexual exploitation of children. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C § 2256) in different forms of media including computer media.

2. I make this affidavit in support of an application for search warrants seeking authorization to search electronic equipment, specifically: a black iPhone ("iPhone"), which contains a SIM[1] card, that is assigned ICC ID[2] number 356842110779316, as well as a SIM card that is assigned ICC ID number 89148000005970515789, and a SIM card that is assigned ICC ID number 89148000006067904159 (hereinafter collectively, the "TARGET DEVICES"), which were all seized from DOMENIQUE DEQUON HINES ("Hines"), year of birth

[1] A SIM (subscriber identity module or subscriber identification module) card is essentially a smart card inside a mobile phone, carrying an identification number unique to the owner, storing personal data, and preventing operation if removed. SIM cards are sometimes removable and sometimes interchangeable – that is, in some circumstances, an individual could remove a SIM card from his phone and insert a different SIM card into that phone in order to access the information contained on the second SIM card.

[2] ICC ID (Integrated Circuit Card Identifier) identifies each SIM internationally. It is inscribed on the back of the SIM Card. A full ICC ID is 19 or 20 characters long and can be thought of as the serial number of the SIM Card. It is also considered as the Issuer's Identification Number.

1997, at his December 3, 2020, arrest in Illinois and remain in the possession of law enforcement, as described in Attachment A. Based on the facts set forth in this affidavit, there is probable cause to believe that the TARGET DEVICES, as described in Attachment A, contain evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 2251(a) and (e), as described in Attachment B.

3. The statements contained in this affidavit are based in part on information provided by FBI Special Agents and other law enforcement officials; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training, and background as a Special Agent with the FBI. Because this affidavit is submitted for the limited purpose of securing authorization for the requested search warrants, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish probable cause.

STATEMENT OF PROBABLE CAUSE

4. On December 1, 2020, a criminal complaint and arrest warrant issued charging Hines, of Illinois, with Sexual Exploitation of Children, in violation of 18 U.S.C. §§ 2251(a) and (e). *See* docket # 20-mj-04300-DHH. The affidavit submitted in support of that complaint is attached hereto as Exhibit 1 and incorporated herein.[3]

[3] On January 12, 2021, a grand jury returned a one count indictment charging Hines with the same offense. *See* docket # 21-cr-10011-WGY.

5. On December 3, 2020, Hines was arrested in Illinois pursuant to the federal arrest warrant issued on December 1, 2020. At the time of Hines' arrest, multiple items were located on his person, including a black iPhone containing one SIM card (that is assigned ICC ID number 356842110779316) that was located on his person as well as two other SIM cards that were in his wallet (collectively, the TARGET DEVICES).

6. In the course of his arrest, Hines was provided with his *Miranda* warnings, which he waived and he consented to an interview. During the interview, Hines provided authorities with the pin code used to unlock the iPhone seized from his person (and described herein and in Attachment A) and provided the telephone number of (XXX) XXX-1013 as the one assigned to his iPhone. Hines stated that he did not recognize the telephone number ending in the last four digits of telephone number (XXX) XXX-3688, which was the number used to communicate with Minor A, as described in Exhibit 1.

7. The iPhone was placed into airplane mode by law enforcement and the TARGET DEVICES were seized by FBI and are currently in the custody of FBI and being stored at its facilities, as described in Attachment A. From my training and experience and the training and experience of law enforcement personnel who routinely handle this type of equipment, I understand that it has been stored in a manner in which its contents are, to extent material to the investigation, in substantially the same state as they were when it first came into agents' possession.

8. In the course of this investigation, I have reviewed records obtained from Verizon Wireless, which identify telephone number (XXX) XXX-3688 and telephone number (XXX) XXX-1013 as being subscribed to by Hines. Telephone number (XXX) XXX-3688 had an

effective date of October 6, 2020 and was changed to inactive on November 7, 2020.[4] The ICC ID assigned to telephone number (XXX) XXX-3688 was 89148000006067904159, which was the same ICC ID located on one of the SIM cards located within Hines' wallet. Records also identified that a silver iPhone 6S 32GB was assigned to telephone number (XXX) XXX-3688.[5]

9. Per Verizon Wireless, telephone number (XXX) XXX-1013 had an effective date of November 7, 2020. A black iPhone SE 20 64GB – *i.e.*, the model seized from Hines at his arrest – was identified by Verizon as being assigned to telephone number (XXX) XXX-1013.

10. In summary, as outlined in Exhibit 1, the investigation has determined that Hines communicated with Minor A, via iMessage,[6] over an approximately ten-day period from a specific telephone number, namely, (XXX) XXX-3688. During the course of their on-line conversations, Hines induced, enticed and coerced Minor A to create and send to him sexually explicit pictures of Minor A. Minor A complied. Further investigation has determined that telephone number (XXX) XXX-3688 corresponds with the SIM card bearing ICC ID 89148000000606790 4159, which was located in Hines' wallet, at the time of his arrest, along with another loose SIM card and an iPhone containing a third SIM card.

CHARACTERISTICS COMMON TO CONSUMERS OF CHILD PORNOGRAPHY

[4] Minor A's parents reported that Hines' communication with Minor A ended on the afternoon of November 6, 2020.
[5] At present, the FBI is unaware of the location of the silver iPhone 6S 32GB.
[6] iMessage is a service provided by Apple that allows users to send texts, documents, photos, videos, contact information, and group messages over the Internet to other users of Apple devices. If a user has multiple Apple devices with the iMessage application installed, he can access his iMessages from any of those devices, regardless of which device was used to send them.

11. Based on my training, experience, and information provided by other law enforcement officers related to investigations involving child pornography, the sexual abuse of children, and other forms of child exploitation, I am aware that individuals who create, possess, receive, distribute, or access with intent to view child pornography – including those who employ, use, persuade, induce, entice or coerce minors to engage in sexually explicit conduct for the purpose of producing child pornography – (collectively, "consumers" of child pornography) have a sexual interest in children and in images/videos of children.[7] Additionally, I am aware that there are certain characteristics common to such consumers of child exploitation material, as outlined in the following paragraphs.

12. The majority of consumers of child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

13. Consumers of child pornography may collect sexually explicit materials, which may consist of hard copy and digital images and videos for their own sexual gratification. These individuals often also collect child erotica, which may consist of images or text that do not rise to the level of child pornography, but which nonetheless fuel their deviant sexual fantasies involving children. Non-pornographic, seemingly innocuous images of minors are often found on computers and digital storage devices that also contain child pornography, or that are used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases,

[7] In 2018, Hines was convicted of Child Pornography/Solicitation of Child out of McHenry County, Illinois. The minor victim in that case was 13 years old. *See* case # 17CF001310.

such images may also assist in determining the origins of a particular child pornography image or series of images.

14. Many consumers of child pornography maintain their sexually explicit materials for several years and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials.[8] They regularly maintain their collections in the privacy and security of their homes, inside their cars, on their person, or in cloud-based online storage. (Indeed, some devices, like phones, thumb drives, and SIM cards, are small enough to effectively keep and conceal on one's person.) Depending on their technical expertise, access to child pornography on seemingly "safe" networks like Tor, or struggle with addiction to child pornography, many consumers of child pornography have been found to download, view, and then delete child pornography on their digital devices on a cyclical and repetitive basis.

15. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[9]

---

[8] *See United States v. Morales-Aldahondo*, 524 F.3d 115, 117-119 (1st Cir. 2008) (3-year delay between last download and warrant application not too long, given affiant testimony that consumers of child pornography value collections and thus often retain them for a period of time, and consumers who use computers to access child pornography are likely to use computers to store their collections).

[9] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

16. Based upon training and experience, I know that persons engaged in the production and possession of child erotica are also often involved in the production and possession of child pornography. Likewise, I know from training and experience that persons involved in the production and possession of child pornography are often involved in the production and possession of child erotica.

17. Based on my training, knowledge, experience, and conversations with others in law enforcement, I understand that an individual who possesses images and/or videos depicting child pornography on one digital storage device and/or Internet email or online storage account is likely to possess child pornography on additional digital storage devices and/or Internet email or online storage accounts that he possesses or controls. Additionally, based on this training and experience, I understand that even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home or other location that is secure, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

18. Based on all of the information contained herein, in addition to the fact that HINES was convicted of Child Pornography/Solicitation of Child in Illinois in 2018 based on an offense involving a 13 years old child, I believe that HINES likely displays characteristics common to consumers of child pornography.

19. I am aware that a SIM card is critical for cell phone use. Without a SIM card, the cell phone cannot connect to a wireless carrier's cellular network. SIM cards store the cell phone number, and other identifying numbers. SIM cards can also store some contacts as

well as text messages. Based on my training and experience, it is not common for an individual to carry multiple SIM cards on his/her person. In this case, HINES was carrying one mobile phone and two additional SIM cards, which implies that the contents of the loose SIM cards were important to him.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

20. I have had training and experience in the investigation of computer-related crimes, including those involving sexual exploitation of children and child pornography. Based on my training and experience, and information provided by other law enforcement officers, I know the following:

(a) Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth."

(b) Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

(c) The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. Electronic storage media of various

types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person, or in his car. Smartphones and/or mobile phones are also often carried on an individual's person.

(d) The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

(e) Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Google, Yahoo!, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer (including smartphones) with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

(f) As is the case with most digital technology, communications by way of computer (including smartphones) can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a

file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

21. Many smartphones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Apple iPhones, such as HINES' phone, are a type of smartphone. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

22. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.

23. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage

medium until it is overwritten by new data. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

24. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, files system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase of delete this evidence because special software is usually required for that task.

25. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache". An Internet browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

26. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the TARGET DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and

malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g.,

running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

27. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

28. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

29. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

30. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From

my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

31. These warrants authorize a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to these warrants in order to locate evidence, fruits, and instrumentalities described in these warrants. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to these warrants, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CONCLUSION

32. Based on the facts set forth in this affidavit, there is probable cause to believe that the TARGET DEVICES, as described in Attachment A, contain evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 2251(a) and (e), as described in Attachment B. I respectfully request that this Court issue search warrants for the TARGET DEVICES authorizing the seizure and search of the items described in Attachment B.

Sworn to under the pains and penalties of perjury,

Lisa A Crandall

Special Agent Lisa A. Crandall
Federal Bureau of Investigation

Sworn to me telephonically in accordance with Fed. R. Crim. P. 4.1 on February 17, 2021. 4:33 P.M.

David H. Hennessy

DAVID H. HENNESSY
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT DISTRICT OF MASSACHUSETTS

-

ATTACHMENT A

Property to be Searched

The TARGET DEVICES were seized from Domenique Dequon Hines on or about December 3, 2020, and are in the custody of FBI Boston, located at its offices at 201 Maple Street, Chelsea, Massachusetts. They are:

1. a black iPhone ("iPhone"), which contains a SIM card that is assigned ICC ID 356842110779316;
2. a SIM card that is assigned ICC ID 89148000005970515789; and
3. a SIM card that is assigned ICC ID 89148000006067904159.

ATTACHMENT B

Description of Information to be Seized

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C §§ 2251(a) and (e), including those related to:

A. The following topics:

1. Child pornography;

2. The sexual abuse or exploitation of children;

3. The identity of any child depicted in videos and photographs located in the equipment or discussed in any communications related to the sexual abuse or exploitation of children; and

4. Minor A.

B. Any communication(s) relating to child pornography, the sexual abuse or exploitation of children, Minor A, or the identity of any child depicted in videos and photographs located in the equipment;

C. The identity of any person who sent or received communication(s) relating to child pornography, the sexual abuse or exploitation of children, Minor A, or the identity of any child depicted in videos and photographs located in the equipment;

D. Any social media account(s) used to send or receive any communication(s) relating to child pornography, the sexual abuse or exploitation of children, Minor A, or the identity of any child depicted in videos and photographs located in the equipment;

E. The travel or whereabouts of DOMENIQUE DEQUON HINES between October 28, 2020 and November 7, 2020;

F. Evidence of who used, owned, or controlled the equipment;

G. Evidence of the times the equipment was used;

H. The identity, location, and travel of any co-conspirators;

I. Passwords, encryption keys, and other access devices that may be necessary to access the equipment;

J. Evidence of the equipment's Internet activity, including IP addresses used to connect to the internet, firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

K. Evidence of the attachment of other hardware or storage media;

L. Evidence of counter forensic programs and associated data that are designed to eliminate data;

M. Contextual information necessary to understand the evidence described in Attachments A and B.

II. Serial numbers and any electronic identifiers that serve to identify the computer equipment.

DEFINITIONS

For the purpose of these warrants:

A. "Equipment" means any hardware, software, storage media, and data.

B. "Hardware" means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone, iPhone and or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for

removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. A "record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.